WE CLAIM:

1. A method for distributed network address translation with security, comprising the following steps:

requesting from a first network device on a first computer network with a first protocol, one or more locally unique security values from a second network device on the first computer network to uniquely identify the first network device during secure communications with a third network device on a second external network and for distributed network address translation with security;

receiving the one or more locally unique security values on the first network device from the second network device with the first protocol; and

storing the one or more locally unique security values on the first network device, wherein the one or more locally unique security values are used to create a secure virtual connection for secure communications with the third network device and for distributed network address translation.

2. A computer readable medium having stored therein instructions for causing a central processing unit to execute the Method of Claim 1.

3. The method of Claim 1 wherein the second network device is a distributed network address translation router.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

4. The method of Claim 1 wherein the one or more locally unique security values are one or more security parameter indexes for an Internet Protocol security protocol.

a2

5. The method of Claim 4 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol or an Internet Key Exchange protocol.

6. The method of Claim 1 wherein the first protocol is a Port Allocation Protocol.

7. The method of Claim 1 wherein the requesting step further includes requesting one or more locally unique ports used to uniquely identify the first network device on the first network for distributed network address translation.

8. The method of Claim 1 wherein the locally unique ports are Port Allocation Protocol ports.

9. A method for distributed network address translation with security, comprising the following steps:

receiving a request message with a first protocol on a second network device for one or more locally unique security values from a first network device;

allocating one of more locally unique security values on the second network device;

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

storing a network address for the first network device with the one or more locally unique security values in a table associated with the second network device, wherein the table is used to maintain a mapping between a network device and one or more locally unique security values for distributed network address translation; and

sending the one or more locally unique security values in a response message with the first protocol to the first network device.

10. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claim 9.

11. The method of Claim 9 wherein the second network device a distributed network address translation router.

12. The method of Claim 9 wherein the one or more locally unique security values include one or more security parameter indexes for an Internet Protocol Security Protocol

13. The method of Claim 10 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol or an Internet Key Exchange protocol.

14. A method for distributed network address translation using security, comprising the following steps:

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

receiving a first message in a second secure protocol on a first network device on a first network to establish a secure virtual connection to the first network device from a third network device on a second external network;

selecting a locally unique security value to use for the secure virtual connection from a list of locally unique security values, wherein the list of locally unique security values was received from a second network device on the first network with a first protocol; and

sending a second message with second secure protocol to establish a secure virtual connection to the first network device on the first network from the third network device on the second external network wherein the second message includes the selected locally unique security value and security certificate sent to the first network device by the second network device.

15. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claim 14.

16. The method of Claim 14 wherein the list of one or more locally unique security values is a list of one or more security parameter indexes for Internet Protocol security protocol.

17. The method of Claim 14 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange Protocol.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

18. The method of Claim 14 wherein the first protocol is a Port Allocation Protocol and the second secure protocol is an Internet Protocol security protocol.

19. The method of Claim 14 wherein the secure virtual connection is an Internet Protocol security protocol security association.

20. A method for distributed network address translation with security, comprising the following steps:

sending a request message in a second secure protocol from a first network device on a first network to a second network device on the first network, wherein the request message in the second secure protocol includes security information;

routing the request message from the second network device to a third network device on a second external network over a secure virtual connection between the first network device and the third network device;

receiving a reply message in the second secure protocol from the third network device on the second network device on the first network for the first network device, wherein the reply message in the second secure protocol includes security information from the request message allocated by the second network device; and

routing the reply message from the second network device to the first network device on the first network using the locally unique ports used for distributed network address translation.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

21. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claim 20.

22. The method of Claim 20 wherein the step of sending a request message in a second secure protocol includes:

constructing a virtual tunnel header for a local network address determined for the second network device;

prepending the virtual tunnel header to the request message, wherein the virtual tunnel header is used to create a virtual tunnel between the first network device and the second network device;

sending the request message to the second network device from the first network device over the virtual tunnel.

23. The method of Claim 20 wherein the step of routing the reply from the second network device to the first network device on the first network using the locally unique port from the reply in the second secure protocol includes:

determining a local network address for the first network device using the locally unique port associated with the second network device;

constructing a virtual tunnel header for the determined local network address for the first network device;

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

prepending the virtual tunnel header to the reply message, wherein the virtual tunnel header is used to create a virtual tunnel between the second network device and the first network device;

forwarding the reply message to the first network device from the second network device over the virtual tunnel.

24. The method of Claim 20 wherein the local network address is an Internet Protocol address and the virtual tunnel header is an Internet Protocol tunnel header.

25. The method of Claim 20 wherein the first protocol is a Port Allocation Protocol and the second secure protocol is Internet Protocol security protocol.

26. The method of Claim 20 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange protocol.

27. The method of Claim 20 wherein the security information includes any of a locally unique security value or a security certificate.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

28. A method for distributed network address translation with security, comprising the following steps:

requesting one or more locally unique ports with a first message from a first protocol on a first network device from a second network device, wherein the one or more locally unique ports are used for distributed network address translation;

requesting one or more locally unique security values with a first message from the first protocol from the second network device, wherein the one or more locally unique security values are used with a second secure protocol to establish a secure virtual connection between the first network device and a third network device on a second external computer network and are used for distributed network address translation with security;

requesting a security certificate on the first network device from the second network device, wherein the security certificate includes a binding between a public encryption key and a combination of a network address for the first network device and the one or more locally unique ports and the second network device provides local security certificate services.

29. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claim 28.

30. The method of Claim 28 wherein the one or more locally unique security values are security parameter indexes from an Internet Protocol security protocol.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

31. The method of Claim 28 wherein the second network device is a distributed network address translation router.

32. The method of Claim 28 further comprising:

establishing a secure virtual connection between the first network device and the third network device on the second external network using the security certificate.

33. The method of Claim 32, wherein the secure virtual connection is an Internet Protocol security protocol security association.

34. A method for distributed network address translation with security features comprising the following steps:

sending one or more locally unique ports allocated on a second network device on a first computer network to a first network device on the first computer network with a second message from a first protocol wherein the one or more locally unique ports are used for distributed network address translator;

sending one or more locally unique security values allocated on the second network device to the first network device with a second message from the first protocol wherein the one or more locally unique security values are used with a second secure protocol to establish a secure virtual connection between the first network device and a third network device on a second external computer network and are used for distributed network address translation with security;

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

sending a security certificate created on the second network device to the first network device, wherein the second network device provides local security certificate services on the first computer network and wherein the security certificate includes a binding for a public encryption key for the first network device and a combination of a network address for the first network device and the one or more locally unique ports allocated to the first network device to authenticate an identity for the first network device for a secure virtual connection between the first network device and a third network device on a second external computer network.

35. A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claim 34.

36. A system for distributed network address translation with security, comprising in combination:

a routing network device for allocating one or more locally unique ports, one or more locally unique security values and security certificates used for distributed network address translation with security for a plurality of other network devices, wherein the second network device provides local security certificate services and routing services for distributed network address translation with security;

a network address table associated with the routing network device for mapping one or more locally unique security values to a network address for a network device; and

a security certificate for binding a public encryption key for a network device and a combination of a network address for the network device and one or more locally unique ports allocated to first network device by the routing network device to authenticate an identity for the

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

network device for a secure virtual connection with external network device on an external computer network, wherein the security certificate is issued by a second network device providing local security certificate services for distributed network address translation with security.

37. The system of Claim 36 wherein the routing network device is distributed network address translation router.

38. The system of Claim 36 wherein the one or more locally unique security values are one or more security parameter indexes for an Internet Protocol security protocol.

39. The system of Claim 36 wherein the secure virtual connection is an Internet Protocol security protocol security association.

McDONNELL BOEHNEN
HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001